الجرائم الإلكترونية " الأهداف - الأسباب - طرق الجريمة ومعالجتها"

اعداد

اسراء جبريل رشاد مرعي

باحثة

الملخص:

إن جرائم الكمبيوتر والانترنت، أو ما يسمى Cyber Crimes هى ظواهر إجرامية تقرع أجراس الخطر لتنبه مجتمعنا عن حجم المخاطر والخسائر التى يمكن أن تنجم عنها، خاصة أنها جرائم ذكية تنشأ وتحدث في بيئة إلكترونية أو بمعنى أدق رقمية، يقترفها أشخاص مرتفعي الذكاء ويمتلكون أدوات المعرفة التقنية، مما يسبب خسائر للمجتمع ككل على المستويات الاقتصادية والاجتماعية والثقافية والأمنية.إذا كانت مجتمعاتنا العربية لم تتأثر بشكل كبير من مثل هذه الظواهر الإجرامية، إلا أن هناك دولا عربية كثيرة أضحت مهتمة بتلك الظواهر، ومفهومها القانوني، وسمات المجرم المعلوماتي، وهو ما سوف نحاول أن نتعرض له بشئ من التفصيل في هذا البحث محاولين أن نضع ولو لبنة صغيرة في الإطار التنظيمي والتشريعي في تلك المسألة.

ABSTRACT:

Cyber Crimes are criminal phenomena that ring the bells of danger to alert our society about the size of the risks and losses that can result from them, especially as they are smart crimes that arise and occur in an electronic environment or in a more precise numerical sense, carried out by intelligent people who possess the tools of technical knowledge , Causing losses to the entire society at the economic, social, cultural and security levels. If our Arab societies were not significantly affected by such criminal phenomena, there are many Arab countries that are interested in these phenomena, their legal concept and the characteristics of the information criminal. And for that we are exposed to in some detail in this research, trying to put even a small brick in the regulatory and legislative framework in that matter.

مقدمة:

تعد الثورة التكنولوجية وبخاصة ثورة الاتصالات أهم التطورات التى يعيشها العالم اليوم، وتعتبر ثورة الاتصالات هى المحرك الأساسي فى التطورات الحادثة فى الوقت الحالي، إلا أنها ليست المحرك الوحيد فى هذه التطورات حيث أن التطور الكبير فى تكنولوجيا الحاسبات قد أسهم بصورة كبيرة فى تسارع معدلات التقدم فى مجال الاتصالات والمعلومات.

وقد كان من نتاج التطور فى الجانبين ظهور أدوات واختراعات وخدمات جديدة فى مختلف المجالات ولقد نتج عن الثورة التكنولوجية تلك ظهور نوع جديد من المعاملات يسمى المعاملات الإلكترونية تختلف عن المعاملات التقليدية التى نعرفها من حيث البيئة التي تتم فيها هذه المعاملات.

ويقصد بالمعاملات الإلكترونية كل المعاملات التى تتم عبر تجهيزات إلكترونية مثل الهاتف، والفاكس، وأجهزة الحواسب، وشبكة الإنترنت، ومؤخراً عن طريق الهاتف المحمول. وتتكون تلك المعاملات من عدد من المكونات الأساسية، يهمنا في هذه الورقة طرح مكون أساسي فيها وهو الجزء الخاص بجرائم تلك المعاملات، أو بمعني أدق القواعد القانونية الجنائية التي تحكم الأفعال التى تتم من خلال أجهزة الحواسب، أو عبر شبكة الانترنت.

إن جرائم الكمبيوتر والانترنت، أو ما يسمى Cyber Crimes هى ظواهر إجرامية تقرع أجراس الخطر لتنبه مجتمعنا عن حجم المخاطر والخسائر التى يمكن أن تنجم عنها، خاصة أنها جرائم ذكية تنشأ وتحدث في بيئة إلكترونية أو بمعنى أدق رقمية، يقترفها أشخاص مرتفعي الذكاء ويمتلكون أدوات المعرفة التقنية، مما يسبب خسائر للمجتمع ككل على المستويات الاقتصادية والاجتماعية والثقافية والأمنية.إذا كانت مجتمعاتنا العربية لم تتأثر بشكل كبير من مثل هذه الظواهر الإجرامية، إلا أن هناك

دولا عربية كثيرة أضحت مهتمة بتلك الظواهر، ومفهومها القانوني، وسمات المجرم المعلوماتي، وهو ما سوف نحاول أن نتعرض له بشئ من التفصيل في هذا البحث محاولين أن نضع ولو لبنة صغيرة في الإطار التنظيمي والتشريعي في تلك المسألة.

مشكلة الدراسة:

في ضوء ما تقدم تتمثل مشكلة هذه الدراسة في الآتي:

التعرف علي الجريمة الإلكترونية وعلاجها وللاجابة عن مشكلة هذه الدراسة ينبغى الاجابة عن هذه الاسئلة:

1- ما هى الجريمة الإلكترونية؟ 2- ما أهداف الجريمة الإلكترونية؟ 3- من هو المجرم المعلوماتى؟ 4- ما هى أدوات الجريمة الإلكترونية؟ 5- ما هي أسباب الجريمة الإلكترونية؟ 6- ما هى طرق الجريمة الإلكترونية؟ 7- ما هى أنواع الجريمة الإلكترونية؟ 8- ما هي خصائص الجريمة الإلكترونية؟ 9- كيف يمكن معالجة الجريمة الإلكترونية؟

المبحث الأول: مفهوم الجريمة الإلكترونية

جرائم الكمبيوتر والانترنت:

تتشابه الجريمة الالكترونية مع الجريمة التقليدية في اطراف الجريمة من مجرم ذي دافع لارتكاب الجريمة وضحية والذي قد يكون شخص طبيعي أو شخص اعتباري وأداة ومكان الجريمة . وهنا يكمن الاختلاف الحقيقي بين نوعي الجريمة ففي الجريمة الالكترونية الاداة ذات تقنية عالية وأيضا مكان الجريمة الذي لا يتطلب انتقال الجانى اليه انتقالا فيزيقيا ولكن في الكثير من تلك الجرائم فان الجريمة تتم عن بعد باستخدام خطوط وشبكات الاتصال بين الجانى ومكان الجريمة.

هذا وتشير مجلة لوس انجلوس تايمز في عددها الصادر في 22 مارس عام 2000 الى أن خسارة الشركات الامريكية وحدها من جراء الممارسات التى تتعرض لها والتى تندرج تحت بند الجريمة الالكترونية بحوالى 10 مليار دولار سنويا وللتأكيد عل جانب قد تغفله الكثير من مؤسسات الأعمال فان نسبة 62 % من تلك الجرائم تحدث من خارج المؤسسة وعن طريق شبكة الانترنت بينما تشكل النسبة الباقية 38% من تلك الخسائر من ممارسات تحدث من داخل المؤسسة ذاتها.

مفهوم الجريمة الالكترونية:

لا يوجد إجماع على تعريف الجريمة الإلكترونية من حيث كيف تُعرف أو ما هي الجرائم التي تتضمنها الجريمة الإلكترونية. وكما يقول فان دير هلست ونيف هناك غياب لتعريف عام وإطار نظري متسق في هذا الحقل من الجريمة وفي أغلب الأحيان تستخدم مصطلحات الافتراضية والحاسوب والإلكترونية والرقمية.

ويتراوح تعريف الجريمة الإلكترونية بين الجرائم التي ترتكب بواسطة الحاسوب إلى الجرائم التي ترتكب بأي نوع من المعدات الرقمية وتعريف الجرائم الإلكترونية باختصار على أنها الجرائم التي ترتكب باستخدام الحاسوب والشبكات والمعدات التقنية مثل الجوال.

تتكون الجريمة الإلكترونية أو الافتراضية (cyber crimes) من مقطعين هما الجريمة (crime) والإلكترونية (cyber) ويستخدم مصطلح الإلكترونية لوصف فكرة جزء من الحاسب أو عصر المعلومات.

أما الجريمة فهي السلوكيات والأفعال الخارجة على القانون والجرائم الإلكترونية هي المخالفات التي ترتكب ضد الأفراد أو المجموعات من الأفراد بدافع الجريمة وبقصد إيذاء سمعة الضحية أو أذى مادي او عقلي للضحية مباشر او غير مباشر باستخدام شبكات الاتصالات مثل الإنترنت (غرف الدردشة – البريد الالكترونية – الموبايل)

وتعتمد تعاريف الجريمة الإلكتروني في الغالب على الغرض من استخدام هذا المصطلح وتشمل عددا محدداً من الأعمال ضد السرية والنزاهة وتوافر بيانات الكمبيوتر أو أنظمة ويمثل جوهر الجريمة الإلكترونية أبعد من هذا الوصف ومع ذلك، فالأعمال ذات الصلة بالحاسوب لأغراض شخصية أو تحقيق مكاسب مالية أو ضرر بما في ذلك أشكال الجرائم المتصلة بالهوية والأفعال المتعلقة بمحتويات الكمبيوترجميعها تقع ضمن معنى أوسع لمصطلح "الجريمة الإلكترونية. "

ولقد عرفها ليوكفيلدت وفنسترا وستول كمصطلح عام لجميع أشكال الجريمة التي تلعب فيها تكنولوجيا المعلومات والاتصالات دورا أساسيا وهنا تقع الكثير من الجرائم ضمن هذا التعريف.

لقد قدم ليوكفيلدت وآخرون قائمة ب ٢٨ جريمة بدءا من قرصنة الأنظمة الرقمية وتثبيت برامج التجسس للاحتيال باستخدام الخدمات المصرفية عبر الإنترنت والمطاردة الافتراضية.

التعريف الدولي للجريمة الإلكترونية

- تعتمد "تعريفات" للجريمة الإلكترونية في الغالب على الغرض من استخدام المصطلح.
- هناك عدد محدود من الأفعال ضد السرية والنزاهة وتوافر بيانات الكمبيوتر أو أنظمته تمثل جوهر الجريمة الإلكترونية
- أعمال متعلقة بالكمبيوتر لتحقيق مكاسب شخصية أو مالية أو ضرر، بما في ذلك أشكال الأفعال المتصلة بجريمة الهوية وجرائم محتويات الكمبيوتر لا تصلح بسهولة إلى الجهود للوصول إلى التعاريف القانونية للمصطلح الكلي.

تعريفات أخري للجريمة الالكترونية

الجريمة الإلكترونية هي كل فعل ضار يأتيه الفرد أو الجماعة عبر استعماله الأجهزة الإلكترونية، ويكون لهذا الفعل أثر ضار على غيره من الأفراد.

الجريمة الإلكترونية هي الجريمة ذات الطابع المادي التي تتمثل في كل سلوك غير قانوني مرتبط بأي شكل بالأجهزة الإلكترونية يتسبب في حصول المجرم على فوائد مع تحميل الضحية خسارة ودائماً يكون هدف هذه الجرائم هو سرقة وقرصنة المعلومات الموجودة في الأجهزة أو تهدف إلى ابتزاز الأشخاص بمعلوماتهم المخزنة على أجهزتهم المسروقة.

الجريمة الالكترونية عبارة عن نشاط اجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الاجرامي.

يعرفها أحمد صياني بأنها تصرف غير مشروع يؤثر في الاجهزة و المعلومات الموجودة عليها وهذا التعريف يعتبر جامع مانع من الناحية الفنية للجريمة الالكترونية حيث انه لارتكاب الجريمة يتطلب وجود اجهزة كمبيوتر زيادة على ربطها بشبكة معلوماتية ضخمة.

لقد عرف الدكتور عبد الفتاح مراد جرائم الانترنت على أنها : " جميع الأفعال المخالفة للقانون والشريعة والتي ترتكب بواسطة الحاسب الآلي من خلال شبكة الانترنت وهي تتطلب إلمام خاص بتقنيات الحاسب الآلي و نظم المعلومات سواء لارتكابها أو للتحقيق فيها ويقصد بها أيضا أي نشاط عير مشروع ناشئ في مكون أو أكثر من مكونات الانترنت مثل مواقع الانترنت وغرف المحادثة أو البريد الالكتروني كما تسمى كذلك في هذا الإطار بالجرائم السيبيرية أو السيبرانية لتعلقها بالعالم الافتراضي، وتشمل هذه الجرائم على :

أي أمر غير مشروع بدءا من عدم تسليم الخدمات أو البضائع مرورا باقتحام الكمبيوتر- التسلل إلى ملفاته - وصولا إلى انتهاك حقوق الملكية الفكرية، والتجسس الاقتصادي (سرقة الإسرار التجارية) والابتزاز عبر الانترنت وتبيض الأموال الدولي وسرقة الهوية والقائمة مفتوحة لتشمل كل ما يمكن تصوره بما يمكن أن يرتكب عبر الانترنت من انحرافات كما تعرف بالجرائم التي لا تعرف الحدود الجغرافية التي يتم

ارتكابها بأداة هي الحاسوب الآلي عن طريق شبكة الانترنت وبواسطة شخص على دراية فائقة.

بينها تعريف الاستاذ: جون فورستر "كل فعل اجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسية و يعرفها مكتب تقييم التقنية بالولايات المتحدة الامريكية انها "الجريمة التي تلعب فيها البيانات الكمبيوترية و البرامج المعلوماتية دورا رئيسيا." وقد عرفتها الدكتورة هدى قشقوش بأنها " كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات. "

آما يعرفها خبراء منظمة التعاون الاقتصادي والتنمية " بأنها " كل سلوك غيرمشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو نقلها. "

والجريمة الإلكترونية لها مسميات عدة منها:

1- جرائم الحاسوب والإنترنت

2- جرائم التقنية العالية

3- الجريمة الإلكترونية

4- الجريمة السايْبِريّة

5- جرائم أصحاب الياقات البيضاء

ومثل تلك الجرائم قد تهدد أمن الدولة وسلامتها المالية والقضايا المحيطة بهذا النوع من الجرائم كثيرة وأبرز أمثلتها الاختراق أو القرصنة وانتهاك حقوق التأليف ونشر الصور الإباحية للأطفال ومحاولات استمالتهم لاستغلالهم جنسيا والتجارة غير القانونية (كتجارة المخدرات) كما تضم انتهاك خصوصية الآخرين عندما يتم استخدام معلومات سرية بشكل غير قانوني.

ولا تقتصر الجرائم الإلكترونية على أفراد أو مجموعات وإنما قد تمتد إلى مستوى الدول لتشمل التجسس الإلكتروني (وأبرز أمثلته ما كشفته تسريبات المتعاقد السابق مع وكالة الأمن الوطني الأميركي إدوارد سنودن، الذي كشف مخططات أميركية عديدة للتجسس ليس على الأفراد فحسب بل على اتصالات دول أخرى) والسرقة المالية وغيرها من الجرائم العابرة للحدود.

وأحيانا توصف الأنشطة التي تتعلق بالدول وتُستهدف فيها دولة أخرى واحدة على الأقل بأنها تقع في إطار "الحرب الإلكترونية"، والنظام القانوني الدولي يحاول تحميل الفاعلين المسؤولية عن أفعالهم في مثل هذا النوع من الجرائم من خلال المحكمة الجنائية الدولية.

أهداف الجرائم الإلكترونية

نستطيع تلخيص بعض أهداف الجرائم الإلكترونية ببضعة نقاط أهمها :

- التمكن من الوصول الى المعلومات بشكل غير شرعي كسرقة المعلومات او الاطلاع عليها او حذفها او تعديلها بما يحقق هدف المجرم.

- التمكن من الوصول عن طريق الشبكة العنكبوتية إلى الأجهزة الخادمة الموفرة للمعلومات وتعطيلها.

- الحصول على المعلومات السرية للجهات المستخدمة للتكنولوجيا كالمؤسسات والبنوك والجهات الحكومية والأفراد وابتزازهم بواسطتها.

-الكسب المادي أو المعنوي أو السياسي غير المشروع عن طريق تقنية المعلومات مثل عمليات اختراق وهدم المواقع على الشبكة العنكبوتية وتزوير بطاقات الائتمان وسرقة الحسابات المصرفية الخ.

المبحث الثاني: المجرم المعلوماتى

المجرم المعلوماتي هو شخص يختلف عن المجرم العادي فلا يمكن أن يكون هذا الشخص جاهلا للتقنيات الحديثة المعلوماتية.

لقد تنوعت الدراسات التي تحدد المجرم، وشخصيته ومدى جسامة جرمه كأساس لتبرير وتقدير العقوبة. ويكمن السؤال في حالتنا تلك كيف يمكن تبرير وتقدير العقوبة في حالة مجرم الكمبيوتر والانترنت وهل هناك نموذج محدد للمجرم المعلوماتي ؟؟ بالتأكيد لا يمكن أن يكون هناك نموذج محدد للمجرم المعلوماتي، وإنما هناك سمات مشتركة بين هؤلاء المجرمين ويمكن إجمال تلك السمات فيما يلي:

- مجرم متخصص: له قدرة فائقة في المهارة التقنية ويستغل مداركه ومهاراته في اختراق الشبكات كسر كلمات المرور أو الشفرات ويسبح في عالم الشبكات ليحصل على كل غالٍ وثمين من البيانات والمعلومات الموجودة في أجهزة الحواسب ومن خلال الشبكات.
- مجرم يعود للإجرام: يتميز المجرم المعلوماتي بأنه يعود للجريمة دائمًا فهو يوظف مهاراته في كيفية عمل الحواسيب وكيفية تخزين البيانات والمعلومات والتحكم في أنظمة الشبكات في الدخول غير المصرح به مرات ومرات فهو قد لا يحقق جريمة الاختراق بهدف الإيذاء وإنما نتيجة شعوره بقدرته ومهارته في الاختراق.
- مجرم محترف: له من القدرات والمهارات التقنية ما يؤهله لأن يوظف مهاراته في الاختراق والسرقة والنصب والاعتداء على حقوق الملكية الفكرية وغيرها من الجرائم مقابل المال.
- مجرم ذكى: حيث يمتلك هذا المجرم من المهارات ما يؤهله للقيام بتعديل وتطويرفي الأنظمة الأمنية حتى لا تستطيع أن تلاحقه وتتبع أعماله الإجرامية من خلال الشبكات أو داخل أجهزة الحواسيب.

فالإجرام المعلوماتي هو إجرام الذكاء ودونما حاجة إلى استخدام القوة والعنف وهذا الذكاء هو مفتاح المجرم المعلوماتي لاكتشاف الثغرات واختراق البرامج المحصنة ويمكن إجمال القواسم المشتركة بين هؤلاء المجرمين في عدة صفات وهي شبه اتفاق بين الكثيرمن الفقهاء شأنها شأن سمات العالم الافتراضي وما يزال الخلاف حول مفاهيم الجريمة المعلوماتية ، والجرائم المستحدثة بصفة عامة وذلك فيما يلي :

- عادة ما تتراوح أعمار تلك الفئة من المجرمين ما بين 18-45 عامًا.
- المهارة والإلمام الكامل والقدرة الفنية الهائلة في مجال نظم المعلومات فمجرمي تلك الفئة ينتمون إلى طبقة المتعلمين والمثقفين ومن لديهم تخصصية التعامل مع أجهزة الحاسب الآلي والقدرة على اختراق التحصينات والدفاعات التي تعدها شركات البرمجة.
- الثقة الزائدة بالنفس والإحساس بإمكانية ارتكابهم لجرائمهم دون افتضاح أمرهم.
- إلمامه التام بمسرح الجريمة وبأدواته ، وبما يجنبه فجائية المواقف التي قد تؤدي إلى إفشال مخططه وافتضاح أمره .
- وتتعدد أنماط الجناة في الجريمة المعلوماتية ، فهناك الهاكارز " Hackers " أو المتسللون وهم عادةً مجرمون محترفون يستغلون خبراتهم وإمكانياتهم في مجال تقنية المعلومات للتسلل إلى مواقع معينة للحصول على معلومات سرية أو تخريب وإتلاف نظام معين وإلحاق الخسائر به بقصد الانتقام أو الابتزاز.

وهناك الكراكرز" " Crackers " المخترقون" سواء كان من الهواة أو المحترفين وعادةً ما يستخدم مجرمو هذا النمط قدراتهم الفنية في اختراق الأنظمة والأجهزة تحقيقاً لأهداف غير شرعية كالحصول على معلومات سرية أو للقيام بأعمال تخريبية. إلخ وهناك العابثون بالشفرات ومؤلفو الفيروسات " Malecions hackers " الخ.

وبينما قد يهدف المجرم المعلوماتي من جريمته إلى تحقيق مكاسب مادية معينة أو إثبات مهارته الفنية وقدرته على اختراق أجهزة الحاسب قد يرتكب مجرمو هذه الفئة

جرائمهم بهدف التسلية أو الترفيه أو لمجرد الرغبة في الإضرار بالغير كالموظف الذي يتم فصله من وظيفته ويلجأ إلى الانتقام منها.

أدوات الجرائم الإلكترونية

حتى يتمكن القراصنة (Hackers) من تنفيذ جريمتهم الإلكترونية يستلزم ذلك توفر أدوات لذلك، ومن أبرزها:

–الاتصال بشبكة الإنترنت وتعتبر أداة رئيسية لتنفيذ الجريمة.
–توفر برمجيات خاصة لنسخ المعلومات المخزنة عند المستخدم على جهاز الحاسوب.
–وسائل التجسس ومنها ربط الكاميرات بخطوط الاتصال الهاتفي.
–البار كود وهي عبارة عن أدوات تستخدم لمسح الترميز الرقمي وفك شيفرة الرموز.
–طابعات.(Printers)
–هواتف رقمية ونقالة.

–برامج ضارة ومنها Trojan horse إذ تتمثل وظيفته بخداع الضحية وتشجيعه على تشغيله فيلحق الضرر الشامل بالحاسوب والملفات الموجودة عليه.

المبحث الثالث: أسباب وأنواع الجريمة الالكترونية

أسباب الجريمة الالكترونية

هناك عدد من الأسباب التي يمكن حصرها كأسباب للجريمة الإلكترونية، منها ما يقع على مستوى كوني،ومنها ما يقع على مستوى مجتمعي، ومنها ما يقع على مستوى فردي أو شخصي. كما ان أسباب الجريمة الإلكترونية تتفاوت وفق نوعها ونوع المستهدف ونوع الجاني ومستوى تنفيذه (فردي، مجتمعي ، كوني). فجرائم الشباب

والهواه والصغار تختلف عن أسباب جرائم المحترفين، وتختلف وفق هدفها سرقة أو معلومات أو تجارة بالمعلومات أو شخصية الخ.

أسباب الجريمة علي المستوي الفردي

1– البحث عن التقدير(sake of recognition)

هناك بعض الجرائم الإلكترونية التي يرتكبها شباب طائش وصغار سن، وذلك من باب التحدي، وحب الظهور في الإعلام. وغالباً ما تتوقف هذه الفئة عن مثل هذه السلوكيات في عمر لاحق بعد سن العشرينيات.

2- الفرصة(Opportunity)

لقد وفرت التقنيات الحديثة والأنترنت فرصاً غير مسبوقة لانتشار الجريمة الالكترونية وتلعب البيئة وترتيباتها دورا كبيرا في إنتاج الجريمة والخروج على قواعد الاجتماعية فوقت الانحراف عن قواعد الامتثال ليلا ونهارا وفي اي مكان وعدم وجود رقابة كلها عوامل تزيد من فرصة ارتكاب الجريمة الإلكترونية وقد تشكل المعلومات هدفاً سهل المنال ويحقق المنفعة السريعة، وبالتالي يمكن سرقتها أو سرقة محتوياتها فهي فرصة مربحة وقليلة المخاطر واحتمالية الكشف للفاعل فيها ضئيلة.

ان تكنولوجيا المعلومات والاتصالات والاستخدام المتزايد للأنترنت قد خلق فرص جديدة للمجرمين وسهلت نمو الجريمة ان جرائم الإنترنت تمثل شكلا جديدا ومميزا للجريمة وقد خلقت تحديات لتوقع التطورات، والوقاية منها.

3- ضبط الذات المنخفض

تنطلق هذه الدراسة من النظرية العامة في السلوك الطائش وتؤكد هذه النظرية أن احتمالية انخراط الأفراد في فعل اجرامي تحدث بسبب وجود الفرصة مع توفر سمة شخصية من سمات الضبط الذاتي المنخفض وقد عرف كل من جتفردستون وهيرشي

السلوك الطائش بأنّه كل فعل يقوم على القوّة والخداع لتحقيق الرغبات الذاتية وبناء على هذا التعريف الذي يستدل على طبيعة السلوك الطائش من خصائص الأشخاص فإن السلوك الطائش يُعدّ مظهرا من مظاهر الضبط الذاتي المنخفض وكما في نظرية الضبط الاجتماعي لهيرشي فالدوافع لارتكاب السلوك الطائش ليست متغيرة وذلك لأن كل فرد قد يندفع لتحقيق مصالحه الشخصية بما في ذلك السلوك الطائش. فالسلوك الطائش يُعدّ عملاً سهلاً وقد يحقِق المصالح الخاصة بسرعة مثل (الرشوة،السرقة) ونحوهما من الأعمال الإجرامية التي تتحقق بسرعة وسهولة دون انتظارٍ أو بذل جهد، ولكن الاختلاف بين الأفراد يعود إلى مستوى ضبط الذات، ووجود الفرصة لارتكاب السلوك المنحرف.

إن توفر صفة الضبط الذاتي المنخفض مع وجود الفرصة لارتكاب السلوك الطائش يعدان عاملين مؤثّرين في ارتكاب السلوك الطائش فتأثير هذين العاملين يكون نتيجة لاتحادهما والتفاعل بينهما هو المؤدّي للسلوك الطائش وقد حاول كلّ جتفردستون وهيرشي عزو الاختلاف بين المجرمين وغيرهم إلى الاختلافات في مستوى ضبط الذات إن نقص ضبط الذات قوة طبيعية تظهر في غياب الخطوات من أجل تطويره أي أنه نتاج للتنشئة الاجتماعية الناقصة حيث يفشل الآباء في مراقبة سلوك الطفل ولا يلاحظون السلوك المنحرف عندما يحدث وإهمال معاقبة الطفل عندما يقترف سلوكاً منحرفاً وعندما يتكوّن الضبط الذاتي في المراحل الأولى عند الأفراد فإن الاختلافات في ضبط الذات تبقى ثابتة بشكل معقول من الوقت الذي تم تحديده عبر أطوار الحياة غير متأثر بالمؤسسات الاجتماعية.

بل على العكس فإن ضبط الذات قد يؤثر على أداء الأفراد في هذه المؤسسات مثل المدرسة والعمل والزواج والأشخاص ذوو الضبط المنخفض لا يميلون إلى السلوكيات المنحرفة فقط، بل إنهم في الأغلب غير ناجحين في المدرسة أو العمل أو الزواج.
أظهرت الدراسات أيضا أن ضبط الذات المنخفض والاستعداد لتحمل المخاطر من أجل تحقيق مكاسب قصيرة الأجل وهذا قد ينطبق على الأفعال التي يمكن ان تسهل أو

تتعزز بواسطة وسائط الاتصالات الإلكترونية والإنترنت بالإضافة إلى ذلك يتعرض الأفراد على الإنترنت لنماذج التعلم الإجرامي والأقران قد يكونون أكثر ميلا للانخراط في الجريمة الإلكترونية ونظرية التعلم الاجتماعي نظرية قد يكون لها تطبيق خاص عندما يتعلق الأمر بالجرائم الإلكترونية فالمجرمين غالبا ما يحتاجون إلى تعلم تقنيات فالنظرية العامة للجريمة ونظرية التعلم الاجتماعي تريان إن الأفراد يتصرفون في البيئة الافتراضية كما يتصرفون في العالم الحقيقي.

4- النشاط الروتيني

ويمكن تفسير زيادة ضحايا الجريمة الإلكترونية من خلال التغييرات في أنشطة الناس الروتينية في الحياة اليومية فمع ظهور شبكة الإنترنت فقد تغيرت طريقة الناس التي يتواصلون فيها أو يتفاعلون مع الآخرين في العلاقات الشخصية والترفيه والتجارة الخ.

ان التغييرات في أنشطة الناس الروتينية مثل استخدام النت وشبكات التفاعل الاجتماعي مثل الفيس بوك والايميل والمواقع وغيرها قد خلقت فرصاً للجناة المتحفزين مع وجود أهداف قيمة وسهلة في الحيز الفضائي مع غياب الحراسة.

يري كوهين وفيلسون أنه من المرجح أن تحدث الجريمة عندما تتلاقي ثلاثة عوامل هي الجانى المتحفز والهدف المناسب وغياب الحراسة أنه لا بد من توافر هذه العوامل الثلاثة من أجل أن تحدث الجريمة وعدم وجود واحد من هذه العوامل هو كافي لمنع حدوث الجريمة.

أسباب الجريمة علي المستوي المجتمعي

1 – التحضر(Urbanization)

يعد التحضر أحد أسباب الجريمة الإلكترونية عامة حيث الهجرة الكبيرة من الريف إلى المدينة وإلى المناطق الحضرية والمدن الكبيرة وعادة ما يهاجر الشباب غير المتمكنين

من مواجهة متطلبات الحياة الحضرية باهضه التكاليف، والتي تتطلب مهارات عالية أحيانا مما يجعل شرائح كبيرة من المهاجرين غير قادرين على تلبية متطلبات الحياة الحضرية مما يجعلهم يعيشون في مدن الصفيح والأحياء الطرفية والهامشية وكنتيجة يجد الناس انفسهم في تنافس غير قادرين على مجاراته مما يجعلهم يلتفتون إلى الاستثمار في الجريمة الإلكترونية حيث لا تتطلب رأس مال كبير والتي تعرف "أولا الياهو"

وكما يرى ميك فان التحضر سبب رئيس للجرائم الإلكترونية في نيجيريا وان التحضر بدون الجريمة مستحيل وكنتيجة فان الصفوة بينهم قد وجدوا إن الاستثمار في الجريمة الالكترونية مربحة.

– 2البطالة (Unemployment)

ترتبط الجريمة الإلكترونية شأنها شأن الجريمة التقليدية بالبطالة والظروف الاقتصادية الصعبة وتتركز البطالة بين قطاعات كبيرة من الشباب وكما يقول المثل النيجيري "العقل العاطل عن العمل هو ورشة عمل للشيطان" ولذا فان الشباب الذين يملكون المعرفة سيستثمرون ذلك في النشاط الإجرامي الإلكتروني.

3- الضغوط العامة (Strains)

تعد الضغوط العامة التي يتعرض لها المجتمع من فقر وبطالة وأمية وظروف اقتصادية صعبة وعوامل ضاغطة على المجتمع عامة وخاصة على قطاع الشباب مما يولد مشاعر سلبية عند شرائح كبيرة من الناس ضد الظروف وضد المجتمع مما يدفعهم إلى أساليب تأقلم سلبية مع هذه الظروف منها الإتجار الإلكتروني بالبشر والجنس والجريمة الإلكترونية وغيرها.

4- البحث عن الثراء(Quest for Wealth)

يسعى الأنسان إلى المتعة ويتجنب الألم هكذا تقول النظرية العامة في الجريمة لجتفردسون وهيرشي ويسعى الناس إلى الوسائل غير المقبولة اجتماعيا لتحقيق أهداف مقبولة اجتماعيا كما ترى نظرية الأنومي لميرتون فالرغبة في الثراء يواجهها صعوبات بالغة في تحقيقه بالطرق المقبولة اجتماعيا والقانونية ولذا يلجأ بعض الناس إلى الجرائم الإلكترونية حيث المستهدف مجتمع أكبر وسهولة التنفيذ وسرعة المردود وقلة الخطورة

5- ضعف إنفاذ القانون وتطبيقه في الجريمة الإلكترونية

(lack of law enforcement and implementation)

هناك الكثير من الدول التي لم تطور تشريعاتها وأجهزة العدالة فيها لكي تتمكن من مجاراة التقدم في الجرائم الإلكترونية وأساليبها وهذا لا يتوقف عند التشريعات وإنما يشمل الشرطة والتحقيق والقضاء وكيفية التعامل مع الأدلة الرقمية على المستوى الوطني كما هو الحالي على المستوى الدولي فمما يشعل الجريمة الإلكترونية غياب التشريعات الجزائية والجنائية وضعف الممارسات العدلية والشرطية والقضائية في محاكمة والتحقيق في الجرائم الإلكترونية وغالباً ما تجد في دول كثيرة تواضع التقنيات المتوافرة وكذلك الخبراء القادرون على متابعة ورصد وملاحقة الجريمة الإلكترونية داخل المجتمع والعابرة منها للحدود الوطنية.

أسباب الجريمة عل المستوي الكونى

1- التحول للمجتمع الرقمي

إن من أهم سمات عصر المعلومات السمات الثلاثة الرئيسة

- تغيرات كمية في مقدار المعلومات المتدفقة ونوعيها، فبفعل تكنولوجيا الاتصالات والمواصلات فأن الصور والمعلومات تغطي كافة المعمورة بسرعة ودقة.

- إرسال المعلومات إلى العديد من الأطراف (البشر والمعدات) فالمعلومات توجه

الصاروخ والصحفي يرسل التقرير والبث المباشر من مكان الحدث.
- وجود الشبكات حيث يتم تداول المعلومات بين جميع الأطراف مثل البريد الإلكتروني الجوال الخ.

لقد دخلنا عصر المعلوماتية الجديدة (أي الفضاء الإلكتروني أو العالم الافتراضي) فالناس يقضون جزءا من حياتهم اليومية في الفضاء الإلكتروني ينشؤون الشبكات والمواقع ويتمتعون بأنواع جديدة من العلاقات الاجتماعية وهم على تواصل مع ما يجري في العالم الخارجي والقيام ببعض الأعمال كل من هذه الأنشطة قد جعلت من الممكن للجميع وبوجود جهاز كمبيوتر أو مودوم مع معرفة التقنية القليلة وبعبارة أخرى فإن شبكة الإنترنت هي من خلقت ما يعرف الآن باسم الفضاء الإلكتروني أو العالم الافتراضى يحتاج المجتمع لكي يقوم بوظائفه إلى أن يعم الأمن والأمان وان يتحقق النظام والاستمرارية ولا يتوقف توفر الأمن والأمان في الواقع المادي للمجتمع بل أنتقل ليشمل العالم الافتراضي.

2- العولمة

ان ظهور "الفضاء الإلكتروني" يخلق ظواهر جديدة متميزة عن وجود أنظمة الكمبيوتر أنفسها والفرص المباشرة للجريمة والتي وفرتها أجهزة الكمبيوتر الآن ضمن الفضاء الإلكتروني قد يظهر الأشخاص الفروق في امتثالهم الخاص (القانوني) وعدم الامتثال (غير القانوني) مقارنة مع السلوك سلوكهم في العالم المادي فالأشخاص، على سبيل المثال، قد يرتكبون جرائم في الفضاء الإلكتروني لا يرتكبونها في الواقع المادي بسبب مكانتهم وموقعهم بالإضافة إلى ذلك، فمرونة الهوية وعدم ظهور الهوية وضعف عوامل الردع تحفز السلوك الإجرامي في العالم الافتراضي.

هذا العصر يتطلب مؤسسات أمنية مصممة للتعامل مع التغير السريع، تركز على الإبداع والشفافية وإرضاء العملاء (المجتمع بأسره)، مؤسسات ذات سرعة عالية في

نشر المعلومات وأعلام الجمهور مؤسسات قادرة علي اعادة تصميم ذاتها لمواجهة المستجدات السريعة والسريعة التغير في عالم الجريمة الالكترونية

3- الترابط الكوني

وهناك عامل يمكن أن يساهم في دفع مستويات الجريمة هو في ظهور الترابط العالمي في سياق تحولات العالم الاقتصادية والديموغرافية. بحلول عام ٢٠٥٠ ، فإن العالم سوف يشهد تضاعف عدد سكان الحضر إلى ٦,٢ مليار – ٧٠ في المائة من سكان العالم المتوقع من ٨,٩ مليار أكد تقرير صدر عن المركز الوطني لجريمة الياقات البيضاء يؤكد أن فضاء الإنترنت قد خلق فرصا جديدة للمجرمين في التواصل مع الضحايا وقد بين أن السمات الفريدة للإنترنت وهي عدم الكشف عن اسم الشخص وسهولة الاستخدام قد وفرت طرق جديدة للمجرمين لارتكاب جرائمهم بالإضافة إلى ذلك يتيح الإنترنت للمجرمين على التواصل بسرعة و بكفاءة نقل كميات كبيرة من المعلومات إلى العديد من الضحايا عبر غرف الدردشة، والبريد الإلكتروني، ولوحات الرسائل، أو مواقع ويب وكل الذي يحتاجونه مهارات الحاسوب الأساسية و أجهزة الكمبيوتر المتصلة بالإنترنت وبناء على ذلك يوفر جهاز كمبيوتر واحد وسائل متنوعة لإجراء مجموعة من الجرائم ويمكن للمجرمين استخدام الكمبيوتر لبدء تواصل مع الضحايا وإدامته عن طريق شبكة الإنترنت لإجراء المعاملات المالية الاحتيالية.

– 4انكشاف البنية التحتية المعلوماتية الكونية

تتفاوت البني التحتية المعلوماتية بدرجة انكشافها إلى الكوارث الطبيعية، والإهمال البشري وسوءالتصرف الإنساني.

حدد التقرير الرئاسي الأمريكي بخصوص حماية البنية التحتية الحساسة خمسة قطاعات بناءً على الخصائص المشتركة لها، وهذه القطاعات هي:

1- قطاع الاتصالات والمعلومات (Information and Communication) وتشمل شبكات الاتصالات العامة (PTN)والإنترنت والحاسبات في المنازل والاستخدام الأكاديمي والحكومي والتجاري.

2- قطاع التوزيع المادي (الفيزيقيPhysical Distributio)) ويشمل الطرق السريعة للمواصلات وخطوط السكك الحديدية والموانئ وخطوط المياه، والمطارات، وشركات النقل، وخدمات الشحن التي تسهل انتقال الأفراد والبضائع.

3- قطاع الطاقة (Energy)

وتشمل الصناعات التي تنتج الطاقة وتوزع الطاقة الكهربائية والبترول والغاز الطبيعي.

4- قطاع المال والبنوك (Banking and Finance) وتشمل البنوك، وشركات الخدمات المالية من غيرالبنوك ونظم الرواتب وشركات الاستثمار والقروض المتبادلة والتبادلات الأمنية والمادية.

5- قطاع الخدمات الإنسانية الحيوية (Vital Human Services) وتشمل نظم التزويد بالمياه، وخدمات الطوارئ والخدمات الحكومية (البطالة والضمان الاجتماعي وتعويض الإعاقات وإدارة سجلات المواليد الخ.(.

أسباب تتعلق بخصائص الجريمة الإلكترونية

فيما يلي مجموعة من خصائص الجرائم الإلكترونية والتي تؤدي إلى ارتكاب الجريمة الإلكترونية منها:

1- الازالة (Removable) الجريمة الإلكترونية لا تتطلب الإزالة فيمكن نسخها فقط.

2- التوافر (Available) المعلومات في كل مكان جاهزة

3- القيمة (Valuable) معلومات بطاقات الائتمان والحسابات المصرفية والتصاميم قيمة.

4- المتعة (Enjoyable) كثير من الجرائم الإلكترونية ممتعة من مثل سرقة الموسيقى والمال.

5- الديمومة (Durable) المعدات والبرامج المسروقة يمكن أن تستخدم لفترة طويلة.

6- سرعة التنفيذ لا يتطلب تنفيذ الجريمة الإلكترونية الوقت الكثير وبضغطة واحدة على لوحة المفاتيح يمكن أن تنتقل ملايين الدولارات من مكان إلى آخر وهذا لا يعنى أنها لا تتطلب الإعداد قبل التنفيذ أو استخدام معدات وبرامج معينة.

7- التنفيذ عن بعد لا تتطلب الجريمة الإلكترونية في أغلبها (إلا جرائم سرقة معدات الحاسب) وجود الفاعل في مكان الجريمة بل يمكن للفاعل تنفيذ جريمته وهو في دولة بعيدة كل البعد عن مكان الجريمة سواء كان من خلال الدخول للشبكة المعنية أو اعتراض عملية تحويل مالية أو سرقة معلومات هامة أو تخريب الخ.

– 8إخفاء الجريمة إن الجرائم التي تقع على الحاسبات الآلية أو بواسطتها)كجرائم الإنترنت) جرائم مخيفة، إلا أنه تلاحظ آثارها والتخمين بوقوعها.

– 9الجاذبية: نظرا لما تمثله سوق المعلومات والحاسب والإنترنت من ثروة كبيرة للمجرمين أو للإجرام المنظم فقد غدت أكثر جذباً لاستثمار الأموال وغسيلها وتوظيف الكثير منها في تطوير تقنيات وأساليب تمكن الدخول إلى الشبكات وسرقة المعلومات وبيعها أو سرقة البنوك أو اعتراض العمليات المالية وتحويل مسارها أو استخدام أرقام البطاقات إلخ.

– 10عابرة للحدود الدولية (Transnational)إن ربط العالم بشبكة من الاتصالات من خلال الأقمار الصناعية والفضائيات والإنترنت جعل الانتشار الثقافي وعولمة الثقافة والجريمة أمرا ممكناً وشائعاً لا يعترف بالحدود الإقليمية للدول ولا بالمكان ولا بالزمان أصبحت ساحتها العالم أجمع

– 11جرائم ناعمة تتطلب الجريمة التقليدية استخدام الأدوات والعنف أحياناً كما في جرائم الإرهاب والمخدرات والسرقة والسطو المسلح إلا أن الجريمة الإلكترونية تمتاز بأنها جرائم ناعمة لا تتطلب عنفاً فنقل بيانات من حاسب إلى آخر أو السطو الإلكتروني على أرصدة بنك ما لا يتطلب أي عنف أو تبادل إطلاق نار مع رجال الأمن.

– 12صعوبة إثباتها تتميز الجريمة الإلكترونية عن الجرائم التقليدية بأنها صعبة الإثبات وهذا ا رجع إلى افتقاد وجود الآثار التقليدية للجريمة وغياب الدليل الفيزيقي (بصمات، تخريب، شواهد مادية) وسهولة محو الدليل أو تدميره في زمن متناه القصر، يضاف إلى ذلك نقص خبرة الشرطة والنظام العدلي وعدم كفاية القوانين القائمة.

أهم طرق الجريمة الإلكترونية

وتشمل وليس حصرا على:

١ – تخريب المعلومات وإساءة استخدامها ويشمل ذلك قواعد المعلومات المكتبات تمزيق الكتب تحريف المعلومات تحريف السجلات الرسمية. الخ.
٢ – سرقة المعلومات ويشمل بيع المعلومات كالبحوث أو الد راسات الهامة أو ذات العلاقة بالتطوير التقني أو الصناعي أو العسكري أو تخريبها أو تدميرها .الخ.
٣ -تزوير المعلومات ويشمل الدخول لقواعد في النظام التعليمي وتغيير المعلومات وتحريفها، مثل تغيير علامات الطلاب.

٤ -تزييف المعلومات وتشمل تغيير في المعلومات على وضع غير حقيقي مثل وضع سجلات شهادات لم تصدر عن النظام التعليمي وإصدارها.
٥ -انتهاك الخصوصية ويشمل نشر معلومات ذات طبيعة خاصة عن الأفراد، أو الدخول لحسابات الأفراد الإلكترونية ونشر معلومات عنهم أو وضع معلومات تخص تاريخ الأفراد ونشرها.

٦ – التصنت وتشمل الدخول لقواعد المعلومات وسرقة المحادثات عبر الهاتف.
٧ – التجسس ويشمل اعتراض المعلومات ومحاولة معرفة ما يقوم به الأفراد.
٨ -التشهير ويشمل استخدام المعلومات الخاصة أو ذات الصلة بالانحراف أو الجريمة ونشرها بشكل القصد منه اغتيال شخصية الأفراد أو الإساءة.
٩ -السرقة العلمية الكتب والبحوث العلمية الأكاديمية وخاصة ذات الطبيعة التجريبية والتطبيقية.

١٠ – سرقة الاختراعات وخاصة في المجالات العلمية لاستخدامها أو بيعها.
١١ – الدخول غير القانوني للشبكات بقصد إساءة الاستخدام أو الحصول على منافع من خلال تخريب المعلومات أو التجسس أو سرقة المعلومات.
١٢ – قرصنة البرمجيات ويشمل النسخ غير القانوني للبرمجيات واستخدامها أو بيعها مرة أخرى.

١٣ – قرصنة البيانات والمعلومات ويشمل اعتراض البيانات وخطفها بقصد الاستفادة منها وبخاصة أرقام البطاقة الائتمانية وأرقام الحسابات وكلمات الدخول وكلمات السر.

١٤ -خلاعة الأطفال وتشمل نشر صور خاصة للأطفال "الجنس السياحي" للأطفال خاصة وللإناث على الشبكات بشكل عام ونشر الجنس التخيلي.
١٥ – القنابل البريدية وتشمل إرسال فيروسات لتدمير البيانات من خلال رسالة إلكترونية.
١٦ -إفشاء الأسرار وتشمل الحصول على معلومات خاصة جداً ونشرها على الشبكة.
– 17الإحتيال المالي بالبطاقات وهذا ناتج عن استخدام غير شرعي لبطاقات التسوق أو المالية أوالهاتف الخ.

١٨ – سرقة الأرقام والمتاجرة بها وخاصة أرقام الهواتف السرية واستخدامها في الاتصالات الدولية أو أرقام بطاقات الائتمان.

١٩ – التحرش الجنسي ويقصد به المضايقة من الذكور للإناث أو العكس من خلال المراسلة أو المهاتفة، أو المحادثة أو الملامسة.

٢٠ – المطاردة والملاحقة والابتزاز وتشمل ملاحقة الذكور للإناث أو العكس والتتبع بقصد فرض إقامة علاقة ما وذلك من خلال استخدام البريد الإلكتروني وإرسال الرسائل.

٢١ – الإرهاب الإلكتروني. يشمل جميع المكونات السالفة الذكر في بيئة تقنية متغيرة والتي تؤثر على فرص الإرهاب ومصادرة هذه التغيرات تؤثر على تكتيكات الإرهاب وأسلحته وأهدافه ومن التكتيكات الإرهابية ما يعرف بالإرهاب الإلكتروني.

أنواع الجريمة الإلكترونية

– 1جريمة إلكترونية تستهدف الأفراد ويُطلق عليها أيضاً مسمى جرائم الإنترنت الشخصية والتي تقتضي على الحصول بطريقة غير شرعية على هوية الأفراد الإلكترونية كالبريد الإلكتروني وكلمة السر الخاصة بهم وكما تمتد لتصل إلى انتحال الشخصية الإلكترونية وسحب الصور والملفات المهمة من جهاز الضحية لتهديده بها وإخضاعه للأوامر، كما تُعتبر سرقة الاشتراك أيضاً من الجرائم ضد الأفراد.
– 2جريمة إلكترونية تستهدف الملكيّة يستهدف هذا النوع من الجريمة الجهات الحكوميّة والخاصة والشخصية ويركّز على تدمير الملفات الهامة أو البرامج ذات الملكية الخاصة ويكون ذلك عبر برامج ضارة يتم نقلها إلى جهاز المستخدم بعدة طرق من أبرزها الرسائل الإلكترونية.

– 3جريمة إلكترونية تستهدف الحكومات وهي هجمات يشنّها القراصنة على المواقع الرسميّة الحكومية وأنظمة شبكاتها والتي تركز جل اهتمامها على القضاء على البنية التحتيّة للموقع أو النظام الشبكي وتدميره بالكامل ومثل هذه الهجمات في الغالب يكون الهدف منها سياسياً.

4- النصب والاحتيال الإلكتروني.

5- الجرائم السياسية الإلكترونية والتي تركز على استهداف المواقع العسكرية لبعض الدول لسرقة المعلومات التي تتعلّق بأمن الدولة.

6- سرقة المعلومات الموثّقة إلكترونياً ونشرها بطرق غير شرعيّة

7- جرائم الشتم والسبّ والقدح

8- جرائم التشهير ويكون هدفها الإساءة لسمعة الأفراد.

– 9جرائم الاعتداء على الأموال أو الابتزاز الإلكتروني.

– 10الوصول إلى مواقع محجوبة.

– 11الإرهاب الإلكتروني.

– 12الجرائم الجنسية الإلكترونية.

– 13جرائم الاعتداء علي الاموال (مؤسسات مصرفية ومالية وبنوك)

خصائص الجرائم الإلكترونية

–تتّسم بسهولة الوقوع في فخها، حيث إنّ غياب الرقابة الأمنية تساهم في انتشارها وتسهيل ذلك.

–الضرر الناجم من الجرائم الإلكترونية غير قابل للقياس إذ إنّها تحلق أضراراً جسيمة.

–صعوبة الكشف عن مرتكب الجريمة إلا بأساليب أمنية وتقنية عالية.

–سلوك خارج عن المألوف وغير أخلاقي مجتمعيّاً.

–ذات عنف وجهد أقل من الجرائم التقليديّة.

–جريمة غير مقيّدة بزمان ومكان إذ تمتاز بالتباعد الجغرافيّ وعدم تقيدها بالتوقيت الزمنيّ.

–سهولة إخفاء آثار الجريمة والأدلة التي تدلّ على الجاني نظراً للترميز والتشفير الذي يحدث على الرموز المخزّنة على وسائط التخزين الممغنطة.

المبحث الرابع : مكافحة الجرائم الإلكترونية

ان الانترنت إختراع بشري يحمل في طياته بدور الشر والخير معا و لم يكن منذ الوهلة الاولى موضوع الحماية المعلوماتية مطروحا حيث كان إستعماله محتكرا من طرف فئة معينة إلا أن إنتشار إستعمال الأنترنت أظهر عيوبا فسجل أول إختراق للشبكة سنة 1988 حيث توقف عملها لمدة ثلاث أيام و لذلك كان لابد من إيجاد برامج أمنية و قواعد قانونية للحماية من الجرائم الإلكترونية.

أولا : الجانب الأمني من الحمايـة

يتعلق هذا الجانب بكل ما هو فني و تقني لحماية شبكة الأنترنت و الكمبيوتر وسوف نطرحه في ثلاث نقاط مسائل تتعلق بأمن المعلومات و مهددات أمن المعلومات و في الأخير الإجراءات الأمنية

1- مسائل تتعلق بأمن المعلومات

يتعلق أمن المعلومات بالمواضيع التالية :

-المسألة الإداريـــة : يوجد في كل مؤسسة كمية هائلة من المعلومات تخزن الحاسوب و نظرا لأهميتها تحتاج إهتمام أمني.

-المسألة الماليـــة : تتمثل في الكلفة المالية المصروفة قصد حماية النظم المعلوماتية و الحاسوبية ذات القيمة الكبيرة.

-المسألة الوظيفية : يجب أن تكون المعلومات جاهزة لإستعمالها عند الحاجة و تكون صحيحة وسرية و كاملة.

-المسألة الخصوصية: يجب حماية النظم الذاتية الخاصة بالأشخاص وإلا سوف يساء إلى الحرية الفردية بإفشائها و التلاعب بها.

-مسألة تحديد مخاطر و حوادث الكمبوتر و الشبكة : هذه الحوادث قد تكون طبيعة أو مفتعلة وتطور تقنيات الحاسوب وإنشاء الإتصالات الحاسوبية يجعل تحديد المخاطر أكثر تعقيدا.

2- مهددات أمن المعلومات

هي الحالة أو الظرف الذي يؤدي حتما إلى تعطيل الشبكة المعلوماتية و أنواع هذه المهددات:

– 1مهددات طبيعيــة : مثل الزلازل التي تؤدي إلى قطع الإتصالات بالشبكة.

– 2مهددات غير مقصـودة من طـرف الإنســان كسوء إستعمال كلمة السر.

3- مهددات إنسانيــة: وهو ما يقــوم به المتسللون الذيــن يخترقون المواقع.

ان الثغرات الأمنية يمكن كشفها من طرف الهاكرز خصوصا في الحواسب الشخصية إما على مستوى خطوط الإتصال فهي معرضة المراقبة بالإشعاعات أو التصنت و التجسس لأنه يستخدم للإتصال بشبكة الأنترنت الألياف البصرية و الأقمار الصناعية كما يمكن إعتراض طريق وصل الأسلاك للإستراق عن طريق الشبكة.

كما توجد ثغرات بروتوكولات الإتصالات في شبكة الأنترنت و كذا الثغرات الموجودة في برامج البريد الإلكتروني e-mail حيث لا يوجد مايمنع من إستعمال و تغير محتوى الرسالة البرامج الخبيثة و لها عدة أنواع مثلا :

1- الفيروسات و حصان طروادة: هذا الأخير يمكن أن يفرغ الملفات من محتوياتها.

2- الباب السري : يسمح بلدخول دون المروربأجهزة أو برامج الحماية.

3- الدودة : برنامج يؤدي إلى تخريب الملفات التي يدخلها.

هذه المهددات وغيرها هي التي تعترض أمن المعلومات والتي لازلت تتطور بتطور العلم.

3- الإجــراءات الأمنيـــة

إن الوقاية هي أمثل الأساليب نفعا في هذه الجرائم و من بينها :

–إستخدام جدار الحماية fire well و هو حاجز يوضع بين الشبكة الداخلي أنترنت و خادم شبكة الأنترنت و من أهم مهامه فحص المعلومات الداخلة و الخارجة و

السماح لها بالمرور في حالة مطابقتها للمواصفات و تقديم تقارير عن التحركات المشبوهة و لكنه يمكن أن يعطل بعض المعلومات و يحدث عطب.

–التشفير و هو تحويل المعلومة من نص واضح إلى آخر غير مفهوم و قد أستحسن هذا النوع من النظام لنجاعته في عدم كشف المعلومات على شبكة الأنترنت.

–التوقيع الرقمي و هي تقنية تفيد في إمكانية عدم تزوير الرسائل الإلكترونية.

–إستخدام أنظمة كشف الإختراقات و وضع حلول للثغرات الأمنية.

–وضع سياسة أمنية للشبكة و حشد كل الإمكانيات البشرية و المادية لتطبيقها.

–الإحتفاظ بنسخ إحتياطية لكل المعلومات الحساسة في أقراص إضافية ليست مرتبطة. بالشبكة.

–تنصيب برامج لمنع ظهور الصور الخلاعية و الإتصال بالمواقع الإرهابية.

–و يرى الدكتور عبد الفتاح مراد في كتابة التحقيق الجنائي الفني ضرورة إستخدام بعض البرامج التي صممت خصيصا للكشف و الوقاية من الفيروس و البعد عن إستعمال كلمة السر البسيطة.

–عند فتح البريد الإلكتروني يجب معرفة من المرسل خشية أن يكون فيروس.

ثانيا : الحلول التشريعية

تمثل هذه الحلول التشريعية في تدابير وقائية تتخدها الدولة و قوانين تسنها من أجل مكافحة هذه الجريمة و حماية المجتمع و لكن لصعوبة التعامل مع هذه الجرائم الجديدة في الوقت الراهن يتطلب الأمر بداية اللجوء إلى حلول قصيرة المدى ثم حلول طويلة المدى و هو إعادة النظر في معظم التشريعات لأن معظم الانترنت أصبح ظاهرة تمس جميع مجالات الحياة.

1- الحلول التشريعية قصيرة المدى

-إن هذه الحلول تتمثل في إصدار السلطة المختصة بعض المراسيم التنظيمية لمقاهي الأنترنت دون إحتكار المعلومة فيمكن في إجراءات إستعجالية فرض بعض الأمور على أصحاب مقاهي الأنترنت.

-وضع البرامج اللازمة لمنع الدخول إلى المواقع المخلة بالحياء و هذا من أهم الظواهر التي برزت في مجتمعنا في ظل غياب التربية السليمة مما يؤدي للإنحلال الخلقي لشبابنا و حتى المراهقين الذي أصبح من السهل عليهم دخول أي موقع يشاءون بالإضافة إلى المواقع الإباحية هناك المواقع الإرهابية و مواقع للعنف كتعليم القتل ، فلا بد من تدبير عاجل لإن الحرية في المعلومة لا تكمن في دخول هذه المواقع.

-وضع برامج للحماية من الفيروسات و هذا كله بمراسيم تنظيمية و يمكن للدولة أن تدعم هذه العملية بتخفيض أسعار هذه البرامج

-التوعية القانونية والتعريف بمدى خطورة الجرائم الإلكترونية.

-إصدار مراسيم من أجل تنظيم تكوين محققين و رجال شرطة و قضاة على التقنية المعلوماتية و المعرفة الكافية لجرائم الانترنت.

-تعريض أشخاص أو مقاهي الأنترنت لغرامة مالية أو حتى إغلاق المقهى إذ تثبت أنه يسمح للمراهقين أو حتى الشباب بالدخول للمواقع السابقة ففي المواد الجنائية لا يمكننا ذكر أكثر من هذا إحتراما لمبدأ لاعقوبة إلا بنص قانوني.

أما من ناحية المواد المدنية و التجارية فإنه :

-يمكن للمحاماة لعب دور مهم لتكييف بعض السلوكيات و المعلومات مع محاولة القضاة تكييف بعض المنازعات التجارية الإلكترونية قياسا على التجارة العادية لحين صدور التشريع المنظم للتجارة الإلكترونية.

- إعتماد حرية الإثبات في المجال التجاري.

-يجب على المشرع أن يوقع بعض المعاهدات لمكافحة الجريمة الإلكترونية.

-يجب على المشرع أن يوقع بعض الإتفاقيات التي تتبنى تعريف التوقيع الإلكتروني و العقد الإلكتروني و مسايرتها بسن قوانينها التنظيمية.

ثانيا : الحلول التشريعية طويلة المدي

-إن الطابع اللامادي و الإفتراضي لشبكة الأنترنت يستلزم تعديل العديد من التشريعات الحالية بالإضافة إلى إستحداث أخرى و هذا لايضطرنا بالضرورة إلى خلق شيء جديد بل يمكننا الإستفادة من الدول الأخرى التي سبقتنا في مجال التشريع لتجريم هذه السلوكيات ما دامت هذه التشريعات لا تخالف النظام العام و الآداب العام و بما أنه لا يمكن معاقبة شخص من دون نص قانوني

الركن الشرعي إذن لابد من سن نصوص قانونية تتناسب و التطور الحالي. و لكننا نلاحظ أنه رغم زيادة إنتشار الجرائم الإلكترونية و فعاليتها إلا أن المشرع لم يضع لحد الآن الإطار القانوني لأي من هذه الظواهر لذا على المشرع أن يعدل أو يصدر قوانين جديدة ففي نطاق الحماية الجنائية يتعين الإقرار بصلاحية المعلومات كمحل للحماية من أنشطة الإعتداء كافة فبدأ بالتشريعة العامة وهي القانون المدني فعلى المشرع أن يعدل فيه بسن تشريع جديد يتضمن الجرائم الإلكترونية و من بينها العقد الإلكتروني و التوقيع الإلكتروني و غيرها من المفاهيم في العالم الإفتراضي الجديد.

-القانون التجاري لقد ظهر في عالمنا اليوم مفهوم جديد هو التجارة الألكترونية و التسويق الإلكتروني و الدفع عن طريق بطاقة الإئتمان و هي مجالات خصبة للإحتيال فلا بد على المشرع أن ينظمها.

-الإثبات و هذا في إعتقادنا من أهم الخطوات التي يجب أن يقوم بها المشرع و هذا بتبني الخبرة و المعاينة كأساليب للتحقيق و إثبات الجريمة الإلكترونية .

–تعديل قانون الإجراءات الجزائية و تعديل قانون حقوق المؤلف و الحقوق المجاورة .

يمكن أن نلخص أساليب مكافحة الجرائم الإلكترونية في الاتي:

–رسم سياسات دولية تفرض عقوبات صارمة على مرتكبي جرائم الإنترنت إذ يستلزم التدخل الحكومي والدولي نظراً للخطورة الجسيمة للأمر.
–الاعتماد على أساليب وتقنيات متطوّرة للتمكن من الكشف عن هوية مرتكب الجريمة والاستدلال عليه بأقل وقت ممكن.

–توعية الأفراد ونصحهم لماهية الجرائم الإلكترونية وكل ما يترتب عليها من مخاطر.

–الحرص على الحفاظ على سرية المعلومات الخاصة بالعناوين الإلكترونية كالحسابات البنكية، والبطاقات الائتمانيّة وغيرها.

–عدم الكشف عن كلمة السر نهائياً وتغييرها بشكل مستمر واختيار كلمات سر صعبة. تجنب تخزين الصور الخاصة بالأفراد على مواقع التواصل الاجتماعي وأجهزة الحاسوب.

–تجنّب تحميل أي برنامج مجهول المصدر.

–استمرارية تحديث برامج الحماية الخاصة بأجهزة الحاسوب ومنها ، MCafee, Norton.

–تأسيس منظمة خاصة لمكافحة الجرائم الإلكترونية والحد منها.

–المسارعة في الإبلاغ للجهات الأمنية فور التعرض لجريمة إلكترونية.
–مواكبة التطورات المرتبطة بالجريمة الإلكترونية والحرص على تطوير وسائل مكافحتها.

–استخدام برمجيات آمنة ونظم تشغيل خالية من الثغرات.

–الحرص على استخدام كلمات سرية للوصول إلى البرامج الموجودة على جهاز الحاسوب.

–عدم ترك جهاز الحاسوب مفتوحاً.

–فصل اتصال جهاز الحاسوب بشبكة الإنترنت في حال عدم الاستخدام.

–أخذ الحيطة والحذر وعدم تصديق كل ما يصل من إعلانات والتأكد من مصداقيتها عن طريق محركات البحث الشهيرة.

–وضع الرقم السري بشكل مطابق للمواصفات الجيدة التي تصعّب من عملية القرصنة عليه من هذه المواصفات بأن يحتوي على أكثر من ثمانية أحرف أن يكون متنوع الحروف والرموز واللغات إلخ.

–يفضل تغيير كلمة المرور الخاصة بك بصفة دورية.

–لا تضع معلومات علي الانترنت لا تحب أن يراها الجميع من تعرفهم ولا تعرفهم وتذكر أنه بمجرد أن تضع معلومات علي الانترنت لن تتمكن أبدا من ارجاعها مرة أخرى حتى لو قمت بحذفها.

–معلوماتك الخاصة (اجعلها خاص) ان معلوماتك الخاصة مثل اسمك بالكامل ورقم هاتفك ورقم الهوية ورقم بطاقتك الائتمان وايضا عنوانك بالتفصيل هي معلومات خاصة لا يجب ان تتاح للجميع علي الانترنت لا شخص لا تعرفه فلا تفصح له عنها او تضعها علي اي موقع لا تثق به.

خاتمة :

ازدهار الحضارة وانتشار التقدم التقني ساعد في تسهيل الكثير والكثير من أمور حياتنا ولكنه في نفس الوقت جلب لنا العديد من المخاطر والأضرار المتعلقة بالحواسيب والشبكة العنكبوتية مما جعل الحكومات والمجتمعات تنتبه إلى ضرورة نشر التوعية

والتعريف بهذه الجرائم عن طريق شرحها وتحليلها للناس وبيان وسائل وطرق الوقاية منها.

وفي الختام نذكر أنه في حالة تعرضك للمضايقة أو التهديد من قبل الاخرين فلا تتردد في اللجوء لخدمة الامن

التوصيات :

–حث الجامعات والمراكز البحثية العربية للبحث والدراسة في الجرائم المعلوماتية والجرائم عبر الانترنت ومحاولة إنشاء دبلومات متخصصة في المجالات الفنية والقانونية المتعلقة بمكافحة تلك الجرائم.

–العمل علي تنمية الكوادر البشرية العاملة في مجالات مكافحة الجرائم المعلوماتية.
–إنشاء مجموعات عمل عربية لدراسة ووضع استراتيجيات وسياسات وإجراءات تنفيذية لمواجهة مثل هذه الجرائم.

–حث جامعة الدول العربية لإصدار قانون نموذجي موحد لمكافحة الجرائم المعلوماتية.

قائمة المراجع:

- البحر، عبد الرحمن (١٩٩٩). معوقات التحقيق في جرائم الأنترنت." رسالة ماجستير غير منشورة" الرياض: أكاديمية نايف العربية للعلوم الأمنية.

- رسالة ماجستير د محمد حجازى عضو مجلس ادارة المركز المصري للملكية الفكرية.

3- http: //droit.moontada.com/t622-topic

4- أنواع الجرائم الإلكترونية http: //mawdoo3.com/

- الجريمة الالكترونية للمؤلف : مصطفى سمارة – مجلة المعلوماتية العدد 29-شهر تموز 2008.